**Практика**

Предлагаю теперь взглянуть на нашу 2 схему с точки зрения технической стороны менеджмента информационной безопасности.

Необходимо решить задачу рационального использования рассмотренных на уроке инструментов.

Исходя из вашей методички и тех знаний, которые вы получили на сегодняшнем уроке, я предлагаю вам сделать 10 минутный тест и направить его мне почтовым сообщением.

Формат теста:

|  |  |  |
| --- | --- | --- |
|  | **ФИО студента:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **№** | **Наименование мер защиты** | **Цели, прикладное размещение (вектор эксплуатации) и необходимость использования** |
| 1 | Применение СКЗИ | Защита персональных данных и конфиденциальной информации. Идентификация и аутентификация пользователя при помощи ЭЦП. Криптографическая защита сетевого трафика. |
| 2 | Подключение SOC центра | Постоянный поиск, мониторинг и анализ вторжений. Проверка сетей компании на уязвимость и анализ инцидентов безопасности. Проактивное предотвращение угроз. |
| 3 | Обеспечение процесса пентестинга | Предназначены для определения уровня информационной безопасности, оценки защищенности и для построения стратегии защиты в целом. Пентесты помогают оценить подверженность корпоративных систем хакерским атакам и оценить возможные риски\угрозы информационной безопасности. |
| 4 | Использование анализаторов кода | Позволяют идентифицировать и предотвратить эксплойты и ошибки (баги) в исходном коде. |
| 5 | Необходимость подключения Anti-fraud | По определенным атрибутам и токенам в режиме реального времени выявляют мошеннические транзакции. |